TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
09/13/2016

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSB16-29)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Flash Player, the most severe of which could allow for remote code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute remote code by luring a victim to visit a specially crafted malicious website. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Adobe Flash Player Desktop Runtime prior to version 23.0.0.162
- Adobe Flash Player Extended Support Release prior to version 18.0.0.375
- Adobe Flash Player for Google Chrome prior to version 23.0.0.162
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 prior to version 23.0.0.162
- Adobe Flash Player for Linux prior to version 11.2.202.635

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Adobe Flash Player is prone to multiple vulnerabilities which could allow an attacker to take control of the affected system.

- An integer overflow vulnerability that could lead to code execution (CVE-2016-4287).
- Multiple use-after-free vulnerabilities that could lead to code execution (CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, CVE-2016-6932).
- Multiple security bypass vulnerabilities that could lead to information disclosure (CVE-2016-4271, CVE-2016-4277, CVE-2016-4278).
- Multiple memory corruption vulnerabilities that could lead to code execution (CVE-2016-4182, CVE-2016-4237, CVE-2016-4238, CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, CVE-2016-6924).

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute remote code by luring a victim to visit a specially crafted malicious website. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:
- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Adobe:
https://helpx.adobe.com/security/products/flash-player/apsb16-29.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4182
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4237
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4238
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4271
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4272
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4274
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4275
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4276
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4277
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4278
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4279
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4280
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4281
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4282
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4283

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4284
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4285
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4287
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6921
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6922
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6923
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6924
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6925
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6926
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6927
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6929
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6930
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6931
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6932